Method and system for blocking undesirable messages

This invention relates to a method and a system for blocking undesirable messages.

Such methods or systems can be used, for example, in mobile radio service systems, such as, for instance the GSM (Global System for Mobile Communications) System.

In addition to voice telephony, the GSM mobile radio system also offers the option to send or to receive short text messages of up to 160 characters in length. This service is known as SMS (Short Message Service) and is described in the technical specifications TS 23.040 Version 5.4.0, Release 5,"Technical Specification Group Terminals; Technical Realization of the Short Message Service (SMS)" of the 3rd Generation Partnership Project (3GPP).

A multimedia capable variant of a mobile messaging service, the so-called MMS (Multimedia Messaging Service) service is currently being standardized for the next generation mobile radio systems (2.5G and 3G) such as, for example, UMTS (Universal Mobile Telecommunication Systems). This MMS Service is specified in the technical specifications TS 22.140 Version 5.2.0, Release 5, "Technical Specification Group Services and Systems Aspects; Service Aspects; Stage 1; Multimedia Messaging Service (MMS)" and TS 23.14 0 Version 5.3.0, Release 5, "Group Terminals; Multimedia Messaging Service (MMS), Functional Description; Stage 2" of the 3rd Generation Partnership Project (3GPP). Messages with a multimedia content will hereinafter be called MMs to differentiate them more clearly from the SMS text messages. As opposed to SMS, there is no limitation placed on pure text content in the MMS. With MMS it will be possible to format texts according to individual taste as well as to embed audio and visual content in a message. Thus an MM can be made up of several MM elements from different file types (e.g. audio or still

frame) or file formats (with the still frame, for example, the so-called "Graphics Interchange Format" GIF or "Joint photographic expert group" JPEG).

Figure 1 shows a known MMS network architecture. Hereinafter a so-called "MMS-User Agent" will be called an MMS UA. The MMS UA can be a software program, for instance on a mobile radio service set or on a device such as laptop or suchlike connected to a mobile radio service set, which realizes MMS. In Figure 1 a distinction is made between a User A and a User B. Correspondingly there is an MMS UA A and an MMS UA B. Hereinafter, with the other network elements, elements A and B are correspondingly differentiated by attaching the letters "A" and "B". Figure 1 further shows two network elements MMS R/S A or MMS R/S B, which represent so-called "MMS Relay/Server". The MMS R/S A or MMS R/S B are network elements which provide the respective MMS UA with MMS functionality in the MMSE (Multimedia Messaging Service Environment) in the area of the responsibility of the MMS Service Provider SP. Correspondingly, Figure 1 shows an MMSE SPA or an MMSE SPB.

A characteristic feature of MMS is that when MMs are delivered between the so-called "Push Mode", whereby an incoming MM is delivered to the recipient immediately, and the so-called "Pull Mode", whereby the recipient is first notified of the arrival of a new MM and can then make his/her own decision as to when or whether he/she downloads this MM to his/her terminal unit. Figures 2 and 3 show the difference between Pull and Push Mode in the delivery of an MM. With the Pull Mode according to Figure 2, first a notification goes from the MMS R/S to the MMS UA to the effect that there is a message, whereas with Push Mode according to Figure 3 the message is transmitted immediately.

Figure 4 shows a known network architecture with defined interfaces for connecting further network elements to an MMS R/S. In addition to the interface MM1, via which the MMS UA and MMS R/S are connected

to each other, as many external computers as desired, i.e. servers, such as, for example, e-mail server, fax server etc. can be connected to an MMS R/S via the interface MM3. The interface MM4 is used to connect external MMS Service Providers. The interface MM5 connects the MMS R/S with the HLR (Home Location Register) of the network operator, in which register the individual subscriber data of each customer is stored. The HRL is thereby within the network operator's area of responsibility. The interface MM6 enables one or several MMS user databases to be connected. Through the interface MM7 it is possible to connect further servers which make value added services from a value added service provider available to MMS users.

The MMS can be individualized if so desired. Based on individual user settings, an MMS R/S can have certain MMs treated in a special way. Thus, for example, MMs that belong to a specific MM category, e.g. personal MMs, can be immediately forwarded by the MMS R/S, i.e. without the MM UA being notified to an e-mail address predetermined by the user. Further, MMs that have specific keywords in the title can also be automatically deleted by the MMS R/S, or MMs that come from a particular sender can be delivered immediately, i.e. in Push Mode, to the MMS UA, while the usual delivery method desired for all other MMs is the Pull Mode. Over and above that, other personal rules are conceivable.

However, all rules have the disadvantage that the MMS user has to have already defined them before the MMs arrive in the MMSE of his/her MMS Service Provider. This can be done either when the contract is made or, during the contract term, by phone or also using (mobile) „web browsing". The individual rules for personalizing the MMS are usually managed in the MMS user database, which the MMS R/S can access via the interface MM6.

In the MMS, a sender also has the option of sending his/her MMs anonymously. Comparisons with other services where the sender can remain anonymous to the recipient, such as, for example, the

traditional letter post, show, however, that in individual cases, misuse can occur in the form of undesirable promotions, offensive material and suchlike. Misuse can also not be excluded with anonymous MMs.

Although the recipient can set up a filter on his/her MMS UA to sort out the MMs that reach him from undesirable senders. However, this has the disadvantage that the filter functionality does not come into play until after transmission of the MM or the notification via the valuable air interface. Depending on the type of account he/she has with his/her service provider, the data that was transmitted contrary to his/her desire is already invoiced to the recipient at this point in time. Further, there is the disadvantage that MMs sent anonymously do not have the filter criteria. There is no known criteria whereby filtering should be done if, for example, the identity of the sender is not known to the MMS UA or if the alias name given can only be assigned to the actual sender temporarily, i.e. only for one single MM.

The object of the invention is thus to provide a method and a system for blocking undesirable messages, said method and system efficiently rejecting undesirable messages and thereby keeps the number of messages to be transmitted via the valuable air interface to a minimum.

This object is achieved according to the invention by a method for blocking undesirable messages, with the features of Claim 1 and a system for blocking undesirable messages, with the features of Claim 14. In addition a terminal unit with the features of the Claim 27 and a transmitting/receiving device with the features of the Claim 28 presents a solution to the task. The respective subclaims define preferred and advantageous embodiments of the present invention.

The method according to the invention for blocking undesirable messages comprises the following steps:

- a message is sent from a sender to a transmitter,
- the message is sent from a transmitter to a service provider, and
- the message is transmitted from the service provider to a recipient, whereby the recipient is served by the service provider.

The message is transmitted from the service provider to the recipient only if the sender does not figure in a list of exclusions. The sender may, for example be an MMS UA and the transmitter an MMS R/S. The recipient is preferably registered with the service provider, in other words, he/she is under contract to the service provider. Using this method, in the future, only messages from senders who do not figure in a list of exclusions will be transmitted to the recipient via the air interface.

Preferably, the list of exclusions is managed by the service provider. This has the advantage that the service provider always knows which senders are excluded from sending to certain recipients or groups of recipients. In a preferred embodiment of the present invention, the list of exclusions is the recipient's personal, i.e. individually compiled list of exclusions. In this case, the service provider manages a personal list of exclusions for each recipient, said list being consulted before an incoming message is transmitted to the recipient via the air interface.

In a further embodiment of this invention, the list of exclusions is a general list of exclusions, which is consulted for all recipients and/or groups of recipients. It is conceivable that a general list of exclusions is managed by the service provider. Senders whose messages should never be sent to any recipient and/or groups of recipients whatsoever via the air interface are put on this list of exclusions. Thereby the service provider can determine according to his own criteria which persons or recipients can put senders on a corresponding general list of exclusions or how the groups of recipients are made up. Personal and general lists of exclusions can also be combined.

In a further development of the present invention the recipient notifies the service provider if he/she wants to have a sender put on the list of exclusions. It is conceivable that the recipient draws up his/her list of exclusions him/herself. To this end, the recipient notifies the service provider which sender he/she wants to have put on the list of exclusions. Alternatively, it is also conceivable that only the service provider itself can have senders put on a list of exclusions.

In a further development of this invention the recipient receives the message anonymously and notifies the service provider if he/she wants to have the sender of the message placed on the list of exclusions. In such a case, the sender is not known to the recipient. If, nevertheless, the recipient does not wish to receive any more messages from this sender, for instance, because the messages are promotional messages, then the recipient can notify the service provider of this. The service provider knows the name of the sender, but just does not pass this name onto the recipient. Thus it is possible for the service provider to place the name of the sender on the list of exclusions.

In a further development of this invention, the recipient receives the message with an alias name and notifies the service provider if he/she wants to have the sender of the message placed on the list of exclusions. Similarly to when messages with an anonymous sender are received, when a message with an alias name is received the recipient does not know who the actual sender is. If, nevertheless, the recipient does not wish to receive any more messages from this sender, then again the recipient can notify the service provider of this, the actual sender being known to the service provider. Accordingly, the service provider can put this sender on the list of exclusions, so that in future the recipient will not receive any more messages from this sender. Thus again the air interface to the recipient is freed.

In a preferred embodiment, the notice to the service provider is formed as a self-contained, i.e. so-called „abstract message". It is further preferred that the notice to the service provider is integrated in the abstract message in the form of an information element.

In a further embodiment, the notice to the service provider is contained in an MM, in particular in the user data of the MM.

The notice to the service provider can also contain further information for the filter functionality, in particular type of the list of exclusions and/or time limitations.

In a preferred embodiment, the notice to the service provider contains an identification signal from which the service provider can determine the identity of the sender. If the recipient has only received the anonymous message or the message with the alias name, the problem arises as to how the recipient can notify the service provider as to which sender should be put on the list of exclusions. In such a case, along with his notice, the recipient sends the service provider an identification signal, by means of which the message or the sender can be unequivocally identified. Thereby, preferably a message identifier and/or the alias name are used as an identification signal. The message identifier can be a reference to the storage location of the message, the so-called URI (Uniform Resource Identifier), from the notification, or it can be a message ID, from the delivery of the MM.

The object set at the beginning is achieved by means of a system for blocking undesirable messages. The system comprises a transmitter that can send a message from a sender, a service provider that can receive the message from the transmitter and a recipient served by the service provider, whereby the recipient can receive the message from the service provider. Thereby the service provider can transmit the message to the recipient only if the sender does not figure in

the list of exclusions.

The present invention further relates to a terminal unit, in particular a mobile radio service terminal unit for use with a method according to the invention and/or for use in a system according to the invention. The present invention further relates to a transmitting/receiving device, in particular a mobile radio service base station for use with a method according to the invention and/or for use in a system according to the invention.

One advantage of this invention is that the incoming MMs can be examined before they are notified or before they are delivered to see whether the sender of the MM figures on a private and/or public list of exclusions of the recipient. By this means the data traffic (especially via the limited resources of the air interface) is reduced, which leads to lower costs.

A further advantage is that even in the event of MMs sent anonymously, a filter functionality is effective as the identity of the sender is known to the MMS Service Provider as opposed to the recipient.

Finally it is advantageous that a recipient can dynamically extend his/her list of exclusions by new entries any time after a notification has been received or after an MM has been delivered.

The invention is explained in more detail below with reference to the attached drawings with the aid of exemplary embodiments. The features illustrated there and the features already described above can be fundamental to the invention not only in the combinations cited but also individually and in other combinations, in which;

Figure 1 shows an MMS network architecture;
Figure 2 shows a diagrammatic view of the Pull Mode;
Figure 3 shows a diagrammatic view of the Push Mode;

Figure 4 shows a diagrammatic view of an MMS R/S and its interfaces;

Figure 5 shows a diagrammatic view of an MM being sent from an MMS UA A to the MMS UA B; and

Figure 6 shows a diagrammatic view an MM being sent anonymously.

The Figures 1 to 4 have already been described in the introduction of the description and so will not be explained again here.

Figure 5 shows an exemplary embodiment of an MM being sent from a user MMS UA A to a user MMS UA B via the network elements MMS R/S A and MMS R/S B. The exchange of data between the data transmission units mentioned is to be described in this exemplary embodiment using the so-called "abstract messages", i.e. short messages defined in the technical specifications TS 23.140 Version 5.3.0, Release 5, "Group Terminals; Multimedia Messaging Service (MMS); Functional Description; Stage 2" of the 3rd Generation Partnership Project (3GPP). An abstract message consists of at least one information element. In the MMS the sender, i.e. the user A can send an MM with the abstract message 1 via the air interface MM1 to the MMS R/S A in the MMSE environment of his/her service provider A. The MMS R/S A confirms the correct receipt of the MM from the MMS UA A with the abstract message 2.

The MM is transmitted to the MMS R/S B in the service area B of the recipient with the abstract message pair 3 (contains the MM) and 4 (response). Thereupon the recipient, i.e. the user B is notified with the abstract message 5 of the MM ready to be downloaded. This notification contains as reference a URI (Uniform Resource Identifier) of the storage location of the MM. The abstract message 6 serves primarily as confirmation that the user MMS UA B has received the notification correctly and to inform the MMS Service Provider of the delivery mode preferred by the recipient, i.e. Push or
Pull Mode. The recipient, i.e. the user B, can initiate the download

of an MM waiting in the MMS R/S B with the abstract message 7. The MM is then delivered from the MMS R/S B to the MMS UA B using the abstract message 8. In addition to the MM itself, this abstract message also contains an identification element, i.e. the so-called message ID, by means of which the MM can be unequivocally referenced later for further MMS functionalities both by the MMS R/S B and by the MMS UA B of the recipient. The MMS R/S B can be informed of the outcome of the download by means of the abstract message 9 from the MMS UA B.

With MMS a sender has the option of sending his/her MMs anonymously. This function is, for example, of advantage when opinion polls are carried out using MMS or advisory services such as, for instance, debt advice, alcoholics anonymous etc. are used. There an information element must be placed accordingly in the abstract message 1 when the MM is sent.

Thereby the address of the sender is only withheld from the recipient of the MM. That means that the address is withheld in the notification concerning a newly arrived MM ready for downloading in the abstract message 5 and when the MM in the abstract message 8 is downloaded. Thereby the MMS Service Providers concerned still have full knowledge of the identity of the sender. This is necessary so that the MMs can be charged accordingly.

In the case of sender anonymity, the MMS Service Provider can either replace the actual address of the sender in the corresponding information element of the abstract messages 5 and 8 concerned with an alias name or leave it empty. Alternatively it is also conceivable that the MMS Service Provider leaves out the corresponding information element.

Figure 6 shows an exemplary embodiment of a message #1 being sent from a sender to a recipient. The sender sends the message #1 to a service provider XY. Although the sender has applied for anonymity,

the address Andreas.Schmidt@XY.de is known to the service provider XY. The service provider XY subsequently notifies the recipient that a message from an anonymous subscriber is waiting. Using a data request command the recipient accesses the storage location at the service provider XY. Then the message is sent with an anonymous sender identifier from the service provider XY to the recipient.

In response to a notification or in response to a MM delivered, the recipient can inform his/her MMS Service Provider that in future he/she does not want to receive any further MMs from the sender of this MM and can do so by sending an appropriate request A to his/her MMS Service Provider. Thereby one must distinguish between two cases:

1. The identity of the sender is not known

If the sender of an MM remains anonymous, then in one embodiment the request A can contain an identification signal I from which the MMS Service Provider can ascertain the identity of the sender. In response to a notification of a new MM ready to be downloaded, the storage location of the MM (URI) contained in the notification (abstract message 5 according to Fig. 5) can be used as identification signal I. If the request A of the recipient is a response to a message delivered (abstract message 8 according to Fig. 5), then the message ID of the MM can be used as identification signal I.

If the MMS Service Provider has replaced the actual address of the sender by a temporary alias name, it is also possible to use this alias name as identification signal I. As, however, according to the technical specification TS 23.140, Version 5.3.0 Release 5 of the 3GPP, the information element for the sender address does not necessarily have to be transmitted, and it might not be possible later to unequivocally assign the alias name conferred temporarily by the MMS Service Provider to the actual sender, URI or message ID

are preferably used as identification signal I.

2. The identity of the sender is known

If the identity of the sender is known, then, as an alternative to the URI (after the notification) or to the message ID (after the MM has been delivered), the address of the sender who is to be placed on the list(s) of exclusions can also be sent to the MMS Service Provider as identification signal I with the request A. As, according to the technical specification TS 23.140, Version 5.3.0 Release 5 of the 3GPP, the information element for the sender address does not necessarily have to be transmitted, it is also the case here that the URI or message ID should preferably be used as identification signal I.

The following table shows which identification signals I can be used in the request A.

Request A as response to	Notification			Delivery		
Sender is	unknown to the recipient		known to the recipient	unknown to the recipient		known to the recipient
Identification signal I	URI	Alias name	Sender address	Message ID	Alias name	Sender address

Further exemplary embodiments of the present invention are explained below. With regard to the messages, reference will be made to the process according to Figure 5. The sending of an MM on the sender's side proceeds as follows: the sender sends an MM with the abstract message 1 via the interface MM1 to the MMS R/S A in the MMS area A of his/her MMS Service Provider, whereby the sender has the option to inform his/her MMS Service Provider whether or that he/she would

like to hide his/her identity from the recipient. The MMS R/S A confirms with the abstract message 2 that the MM has been received correctly. The MM is sent, if necessary with the abstract message pair 3 (contains the MM) and 4 (contains a response) to the MMS R/S B in the MMS area B of the recipient.

In the following exemplary embodiment it is assumed that the recipient is notified of the identity of the sender and that the request A is a response to the MM notification. After the MM has been received in the area of responsibility MMSE B of the MMS Service Provider SP B, first the abstract message 5 notifies the recipient that there is an MM ready to be downloaded. This notification contains the address of the sender (optional), and also the URI (reference to the storage location) of the MM (obligatory). The abstract message 6 serves primarily as confirmation that the MMS UA B received the notification correctly.

The recipient recognizes from the subject and/or the address of the sender that it involves a promotional offer that is of no interest to him/her, and, therefore, the sender sends a request A to his/her MMS Service Provider to have the address of the sender put on a so-called "black list", whereby the sender address from the notification is used as identification signal I. The MMS Service Provider SP can put this sender address directly on the personal "black list" of the recipient. In the future, the MMS Service Provider of the recipient deletes further MMs from this sender and said MMs are not offered to the recipient for downloading any more. Hence the recipient is no longer bothered by undesirable messages from the sender.

In a further exemplary embodiment it is assumed that the identity of the sender will not be imparted to the recipient, that the information element for the sender address is missing and that the request A is a response to the MM notification. After the MM has been received in the area of responsibility MMSE B of the MMS

Service Provider B, first the abstract message 5 informs the recipient that there is an MM ready to be downloaded. There is no sender address in this notification as the sender expressed the wish for anonymity. However, the notification contains a reference (optional) and the URI (reference to the storage location of the MM, obligatory). Thereby, the abstract message 6 serves primarily as confirmation that the MMS UA B has received the notification correctly.

In this exemplary embodiment, the recipient recognizes from the subject or reference line that it involves a promotional offer that is of no interest to him/her, and, therefore, the recipient sends a request A to his/her MMS Service Provider to have the address of the sender put on a so-called "black list", whereby the URI of the MM from the notification is used as identification signal I. The MMS Service Provider can ascertain the identity of the sender from the URI and put it on the personal black list of the recipient. In the future, the MMS Service Provider of the recipient deletes further MMs from this sender and said MMs are not offered to the recipient for downloading any more. Hence the recipient is no longer bothered by undesirable messages from this sender.

In a further exemplary embodiment it is assumed that the recipient is not notified of the identity of the sender, that the sender address contains an alias name and that the request A is a response to the delivery of the MM. After the MM has been received in the area of responsibility MMSE B of the MMS Service Provider B, first the abstract message 5 informs the recipient that there is an MM ready to be downloaded. In this exemplary embodiment the notification also contains an alias name (e.g. Anonymous.Subscriber@XY.de") as sender address in addition to the URI (reference to the storage location). The abstract message 6 serves primarily as confirmation that the MMS UA B has received the notification correctly.

The recipient decides to download the MM on the basis of the information contained in the notification. The MMS UA B sends the abstract message 7 to the MMS R/S B to initiate the download of the MM. The MMS R/S B delivers the MM to the MMS UA B by means of the abstract message 8. In addition to the MM (i.e. the multimedia user data) an alias name (e.g. "Anonymous.Subscriber@XY.de") as sender address and a message ID for the MM are sent with the abstract message 8. The MMS R/S B can be informed of the successful outcome of the download by means of the abstract message 9 from the MMS UA B. If the recipient determines that his/her decision to download the MM was a mistake, as, instead of useful information, the MM only contains offensive material, he/she can now direct a request A to his/her MMS Service Provider to have the sender address put on a black list, whereby the (obligatory) message ID of the MM from the abstract message 8 is used as identification signal I. The MMS Service Provider SP B can ascertain the identity of the sender from the message ID and put this sender on the personal black list of the recipient. In the future, the MMS Service Provider of the recipient deletes further MMs from this sender and said MMs are not offered to the recipient for downloading any more. Hence the recipient is no longer bothered by undesirable messages from the sender and no unnecessary data is sent via the air interface to the recipient B.

Several possibilities lend themselves to sending the request A from the MMS UA B of the recipient to the MMS R/S B of the MMS Service Provider SP B, and these are described below.

The request A can be sent as a self-contained abstract message, which (in addition to other information) also contains the identification signal I as a self-contained information element. Other information could be, for example, further filter criteria, the statement of the corresponding list (e.g. private or public) or time limitations for the desired filter functionality.

Furthermore the request A can also be sent as a self-contained

information element in an already known abstract message defined by the 3rd Generation Partnership Project (3GPP), for example, in the so-called "MM1_notification.RES" (Ref. 6), "MM1_retrieve.REQ" (Ref. 7), "MM1_acknowledgement.REQ" (Ref. 9) shown in illustration 5 or also in the abstract message "MM1_read_reply_recipient.REQ" (used to send a read confirmation of the recipient) not shown in illustration 5.

Finally, the request A can also be sent as user data within an MM that is ideally addressed to a service address of the MMS Service Provider for updating black lists.

The black list(s) should preferably be managed in the area of responsibility MMSE of the MMS Service Provider SP, so that the filter functionality is already effective before further MMs from the same sender are sent via the valuable air interface. Thereby the black list can preferably be incorporated as part of the MMS user database via the interface MM6 into the MMSE of the MMS Service Provider SP (cf. Figure 4). Alternatively, however, the black list can also be managed on a separate computer or by the MMS R/S directly.